



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,661	01/28/2002	James F. Riordan	CH9-2000-0011	8370

29683 7590 06/21/2005

HARRINGTON & SMITH, LLP
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER

CERVETTI, DAVID GARCIA

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/058,661

Applicant(s)

RIORDAN ET AL.

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 28 January 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-13 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-13 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 28 January 2002 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 5/15/02.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed May 15, 2002 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 1 (figure 1). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The abstract of the disclosure is objected to because it exceeds 150 words in length. Correction is required. See MPEP § 608.01(b).

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

4. The disclosure is objected to because of the following informalities: "DES" (page 1, line 31), "IDEA" (page 7, line 32). While well known in the art, these terms have not been defined.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 9 recites the limitation "switching to one of said second cryptographic algorithms" in line 2 of the claim. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 12 recites the limitation "computer software product as claimed in claim 10" in line 1 of the claim. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. **Claims 1, 3, 5, 7-8, 10-11, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. (US Patent Number: 6,327,661), and further in view of Tschudin (NPL Apoptosis – the Programmed Death of Distributed Services”).**

Regarding claim 1, Kocher et al. teach a cryptographic system comprising first cryptographic algorithm means for enabling cryptographic operations (column 2, lines 60-67, column 13, lines 20-67), input/output means for receiving input streams and sending output streams (column 13, lines 20-67, column 14, lines 61-67), wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67), at least one test plaintext P_i and for each test plaintext P_i a corresponding test ciphertext C_i (column 13, lines 20-67), receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 1-60), checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under the cryptographic operation of said first cryptographic algorithm means (column 13, lines 20-67), switching means for stopping said cryptographic operations with said first cryptographic algorithm means (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said

checking means (column 13, lines 20-67). Kocher et al. do not expressly disclose including at least one apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 3, Kocher et al. teach said receiving means is made for accepting control streams which include at least one plaintext P_i , for each plaintext P_i a corresponding ciphertext C_i (column 2, lines 60-67, column 3, lines 1-10) and said checking means is made for trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , wherein said checking is done with said apoptosis key of said equal test plaintext P_i and said equal test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67). Kocher et al. do not expressly disclose a corresponding apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 5, Kocher et al. teach a method for creating a cryptographic system for carrying out cryptographic operations characterized by the steps of

Art Unit: 2136

implementing within said cryptographic system a first cryptographic algorithm enabling said cryptographic operations (column 2, lines 60-67, column 3, lines 1-10), selecting at least one test plaintext P_i and enciphering each test plaintext P_i with said first cryptographic algorithm thereby generating a corresponding test ciphertext C_i for each test plaintext P_i (column 2, lines 60-67, column 13, lines 20-67), implementing within said cryptographic system said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67), implementing within said cryptographic system receiving means for receiving a control stream (column 13, lines 20-67, column 14, lines 61-67), implementing within said cryptographic system checking means for checking whether said at least one test ciphertext C_i is the enciphered image of the corresponding test plaintext P_i under said first cryptographic algorithm (column 13, lines 20-67), implementing within said cryptographic system switching means for stopping said cryptographic operations with said first cryptographic algorithm (column 13, lines 20-67), wherein said stopping by said switching means is triggered by said checking means (column 13, lines 20-67). Kocher et al. do not expressly disclose the use of one apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 7, the combination of Kocher et al. and Tschudin does not expressly disclose publishing said at least one test plaintext P_i and for each test plaintext P_i said corresponding test ciphertext C_i . However, Examiner takes Official Notice that publishing information was conventional and well known at the time the invention was made. Furthermore, Kocher et al. stores plaintext and ciphertext prior to comparing them. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to publish this information since Examiner takes Official Notice that it was conventional and well known.

Regarding claim 8, Kocher et al. teach a method for operating a cryptographic system for carrying out cryptographic operations (column 2, lines 60-67, column 3, lines 1-10) characterized by the steps of providing a first cryptographic algorithm for enabling said cryptographic operations (column 2, lines 60-67, column 13, lines 20-67), receiving input streams and sending output streams wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67, column 14, lines 61-67), receiving a control stream, checking whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i (column 13, lines 20-67), stopping said cryptographic operations with said first cryptographic algorithm, if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm (column 13, lines 20-67). Kocher et al. do not expressly disclose the use of one apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security

(sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 10, Kocher et al. teach wherein said receiving of a control stream includes for each key K_i receiving of a plaintext P_i and a corresponding ciphertext C_i (column 2, lines 60-67, column 3, lines 1-10), and said checking includes trying to find a test plaintext P_i and a test ciphertext C_i equal to said received plaintext P_i , and said received ciphertext C_i wherein said checking is done with said key of said equal test plaintext P_i and said equal test ciphertext C_i (column 13, lines 20-67, column 14, lines 61-67). Kocher et al. do not expressly disclose an apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 11, Kocher et al. teach a computer software product for operating a cryptographic system for carrying out cryptographic operations (column 14, lines 5-60), said product is characterized by a computer-readable medium in which program instructions are stored (column 14, lines 5-60), which instructions, when read by a computer, enable the computer to perform a first cryptographic algorithm that is

Art Unit: 2136

enabling said cryptographic operations (column 2, lines 60-67, column 3, lines 1-10), receive input streams and send output streams wherein said input streams are transformed to said output streams by said cryptographic operations (column 13, lines 20-67, column 14, lines 61-67), receive a control stream which is including at least one key K_i , check whether a test ciphertext C_i is the enciphered image of a corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i , stop said cryptographic operations with said first cryptographic algorithm (column 13, lines 20-67), if said test ciphertext C_i is the enciphered image of said corresponding test plaintext P_i under said first cryptographic algorithm when using said key K_i (column 13, lines 20-67). Kocher et al. do not expressly disclose the use of one apoptosis key K_i . Kocher et al. teach self-destructing keys. However, Tschudin teaches the concept of "apoptosis" related to distributed services and computer security (sections 3-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an "apoptosis key". One of ordinary skill in the art would have been motivated to perform such a modification to control the execution of services (Tschudin, sections 4-5).

Regarding claim 13, the combination of Kocher et al. and Tschudin teaches the limitations as set forth under claim 8 above. Furthermore, Kocher et al. teaches computer program comprising program code means for performing the steps of claim 8 when said program is run on a computer (column 14, lines 5-60).

10. Claims 2 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claim 1 above, and further in view of Esserman et al. (US Patent Number: 5,144,664).

Regarding claim 2, the combination of Kocher et al. and Tschudin does not expressly disclose at least one second cryptographic algorithm means, wherein said switching means enables switching to said at least one second cryptographic algorithm means. However, Esserman et al. teach at least one second cryptographic algorithm means, wherein said switching means enables switching to said at least one second cryptographic algorithm means (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch between multiple encryption algorithms when an encryption algorithm is compromised. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman et al., column 1, lines 39-67, column 2, lines 1-68).

Regarding claim 4, the combination of Kocher et al. and Tschudin does not expressly disclose a cascaded list of different cryptographic algorithm means. However, Esserman et al. teach a cascaded list of different cryptographic algorithm means (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a cascaded list of different cryptographic algorithm means. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman et al., column 1, lines 39-67, column 2, lines 1-68).

11. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claim 5 above, and further in view of Esserman et al.

Regarding claim 6, the combination of Kocher et al. and Tschudin does not expressly disclose implementing within said cryptographic system at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means to said at least one second cryptographic algorithm. However, Esserman et al. teach implementing within said cryptographic system at least one second cryptographic algorithm for said ciphering operations, and switching by said switching means to said at least one second cryptographic algorithm (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use at least one second cryptographic algorithm for said ciphering operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman et al., column 1, lines 39-67, column 2, lines 1-68).

12. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claim 8 above, and further in view of Esserman et al.

Regarding claim 9, the combination of Kocher et al. and Tschudin does not expressly disclose switching to one of said second cryptographic algorithms for said cryptographic operations after said stopping. However, Esserman et al. teach switching to one of said second cryptographic algorithms for said cryptographic operations after

Art Unit: 2136

said stopping (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a second cryptographic algorithm for said ciphering operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a modification to maintain secure communications (Esserman et al., column 1, lines 39-67, column 2, lines 1-68).

13. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. and Tschudin as applied to claim 11 above, and further in view of Esserman et al.

Regarding claim 12, the combination of Kocher et al. and Tschudin does not expressly disclose computer software product, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to said at least one second cryptographic algorithms for said cryptographic operations after said stopping. However, Esserman et al. teach computer software product, wherein said instructions, when read by a computer, enable the computer to perform at least a second cryptographic algorithm and switch to said at least one second cryptographic algorithms for said cryptographic operations after said stopping (column 4, lines 1-41). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a second cryptographic algorithm for said cryptographic operations, and switching to a second cryptographic algorithm. One of ordinary skill in the art would have been motivated to perform such a

Art Unit: 2136

modification to maintain secure communications (Esserman et al., column 1, lines 39-67, column 2, lines 1-68).

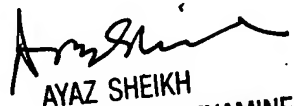
Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100